

Judge Pechman



06-CR-00042-PLAGR

FILED \_\_\_\_\_ ENTERED \_\_\_\_\_  
LODGED \_\_\_\_\_ RECEIVED \_\_\_\_\_

MAY - 4 2006

AT SEATTLE  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
BY \_\_\_\_\_

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

CHRISTOPHER MAXWELL,

Defendant.

NO. CR06-0042P

PLEA AGREEMENT

The United States of America, by and through John McKay, United States Attorney for the Western District of Washington, and Kathryn A. Warma, Assistant United States Attorney for said District, and the defendant, CHRISTOPHER MAXWELL, and his attorney, Steve Bauer, enter into the following Agreement, pursuant to Federal Rule of Criminal Procedure 11(c):

1. The Charge. Defendant, having been advised of the right to have this matter tried before a jury, agrees to waive that right and enter a plea of guilty to the following charges contained in the Indictment. By entering this plea of guilty, Defendant hereby waives all objections to the form of the charging document.

a. Conspiracy, as charged in Count 1, in violation of Title 18, United States Code, Section 371.

b. Intentionally Causing and Attempting to Cause Damage to a Protected Computer, as charged in Count 2, in violation of Title 18, United States

1 Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(B)(ii), 1030(b),  
2 1030(c)(4)(A), and 2.

3 Defendant further understands that before entering his plea of guilty, Defendant  
4 will be placed under oath. Any statement given by Defendant under oath may be used  
5 by the government in a prosecution for perjury or false statement.

6  
7 2. Elements of the Offenses. Defendant understands and acknowledges that  
8 the charges to which he is pleading guilty consist of the following elements:

9 a. Conspiracy

10 First, Defendant agreed with at least one other person to commit  
11 the crime of intentionally causing damage to a protected computer or computer fraud;

12 Second, Defendant became a member of the conspiracy knowing of  
13 at least one of its objects and intending to help accomplish it; and

14 Third, one of the members of the conspiracy performed at least one  
15 overt act for the purpose of carrying out the conspiracy.

16 b. Intentionally Causing and Attempting to Cause Damage to a  
17 Protected Computer

18 First, Defendant knowingly caused the transmission of a program,  
19 information, code, or command;

20 Second, as a result of that conduct, Defendant intentionally and  
21 without authorization caused damage, that is, impairment to the integrity or availability  
22 of data, a program, a system, or information, on, to, or in a computer used in interstate  
23 or foreign commerce or communication; and

24 Third, by that conduct, Defendant caused or attempted to cause a  
25 loss to one or more persons during any one year period aggregating at least \$5,000.00  
26 in value, or, by which conduct Defendant caused the modification and impairment, or  
27 potential modification and impairment, of the medical examination, diagnosis,  
28 treatment, or care of one or more individuals.

1           3.     The Penalties. Defendant understands that the statutory penalties for the  
2 offenses to which he is pleading guilty are as follows:

3               a.     Conspiracy: imprisonment for up to five (5) years, a fine of up to  
4 two hundred fifty thousand dollars (\$250,000.00), a period of supervision following  
5 release from prison of between one (1) and three (3) years, and a one hundred dollar  
6 (\$100.00) penalty assessment.

7               b.     Intentionally Causing and Attempting to Cause Damage to a  
8 Protected Computer: imprisonment for up to ten (10) years, a fine of up to two  
9 hundred fifty thousand dollars (\$250,000.00), a period of supervision following release  
10 from prison of between one (1) and three (3) years, and a one hundred dollar (\$100.00)  
11 penalty assessment, (for a total penalty assessment on the two counts of two hundred  
12 dollars (\$200.00)).

13               Defendant agrees that the penalty assessment shall be paid at or before the  
14 time of sentencing.

15               Defendant understands that in addition to any term of imprisonment  
16 and/or fine that is imposed, the Court may order Defendant to pay restitution to any  
17 victim of the offense, as required by law.

18               Defendant agrees that any monetary penalty the Court imposes, including  
19 the special assessment, fine, costs or restitution, is due and payable immediately, and  
20 further agrees to submit a completed Financial Statement of Debtor form as requested  
21 by the United States Attorney's Office.

22               Defendant understands that supervised release is a period of time  
23 following imprisonment during which he will be subject to certain restrictions and  
24 requirements.

25               Defendant further understands that if supervised release is imposed and he  
26 violates one or more of its conditions, he could be returned to prison for all or part of  
27  
28

1 the term of supervised release that was originally imposed. This could result in  
2 Defendant serving a total term of imprisonment greater than the statutory maximum  
3 stated above.

4  
5 4. Rights Waived by Pleading Guilty. Defendant understands that, by  
6 pleading guilty, he knowingly and voluntarily waives the following rights:

- 7 a. The right to plead not guilty, and to persist in a plea of not guilty;
- 8 b. The right to a speedy and public trial before a jury of Defendant's  
9 peers;
- 10 c. The right to the effective assistance of counsel at trial, including, if  
11 Defendant could not afford an attorney, the right to have the Court appoint one for  
12 Defendant;
- 13 d. The right to be presumed innocent until guilt has been established at  
14 trial, beyond a reasonable doubt;
- 15 e. The right to confront and cross-examine witnesses against  
16 Defendant at trial;
- 17 f. The right to compel or subpoena witnesses to appear on  
18 Defendant's behalf at trial;
- 19 g. The right to testify or to remain silent at trial, at which trial such  
20 silence could not be used against Defendant; and
- 21 h. The right to appeal a finding of guilt or any pretrial rulings.

22  
23 5. United States Sentencing Guidelines. Defendant understands and  
24 acknowledges that, at sentencing, the Court must consider the sentencing range  
25 calculated under the United States Sentencing Guidelines, together with the other  
26 factors set forth in Title 18, United States Code, Section 3553(a), including: (1) the  
27 nature and circumstances of the offense; (2) the history and characteristics of the  
28 defendant; (3) the need for the sentence to reflect the seriousness of the offense, to

1 promote respect for the law, and to provide just punishment for the offense; (4) the  
2 need for the sentence to afford adequate deterrence to criminal conduct; (5) the need for  
3 the sentence to protect the public from further crimes of the defendant; (6) the need to  
4 provide the defendant with educational and vocational training, medical care, or other  
5 correctional treatment in the most effective manner; (7) the kinds of sentences  
6 available; (8) the need to provide restitution to victims; and (9) the need to avoid  
7 unwarranted sentence disparity among defendants involved in similar conduct who have  
8 similar records. Accordingly, Defendant understands and acknowledges that:

9 a. The Court will determine Defendant's applicable Sentencing  
10 Guidelines range at the time of sentencing;

11 b. After consideration of the Sentencing Guidelines and the other  
12 factors in Title 18, United States Code, Section 3553(a), the Court may impose any  
13 sentence authorized by law, including a sentence that, under some circumstances,  
14 departs from any applicable Sentencing Guidelines range up to the maximum term  
15 authorized by law;

16 c. The Court is not bound by any recommendation regarding the  
17 sentence to be imposed, or by any calculation or estimation of the Sentencing  
18 Guidelines range offered by the parties, or by the United States Probation Department;  
19 and

20 d. Defendant may not withdraw a guilty plea solely because of the  
21 sentence imposed by the Court.

22  
23 6. Ultimate Sentence. Defendant acknowledges that no one has promised or  
24 guaranteed what sentence the Court will impose.

25  
26  
27 7. Restitution. Defendant shall make restitution to Northwest Hospital in the  
28 amount of one hundred fourteen thousand dollars (\$114,000.00), and to the United

1 States Department of Defense in the amount of one hundred thirty-eight thousand  
2 dollars (\$138,000.00), with credit for any amounts already paid. Said amounts shall be  
3 due and payable immediately and shall be paid in accordance with a schedule of  
4 payments as set by the United States Probation Office and ordered by the Court.  
5

6 8. Statement of Facts. The parties agree on the following facts in support of  
7 Defendant's guilty plea and for purposes of calculating the base offense level of the  
8 Sentencing Guidelines. Defendant admits he is guilty of the charged offenses.

9 a. CHRISTOPHER MAXWELL was, at all material times, a resident  
10 of Vacaville, California, where he engaged in the conduct described below by accessing  
11 the Internet by and through computers likewise situated in California.

12 b. Northwest Hospital is and, at all material times, was a 187 bed,  
13 community-based, not-for-profit hospital located in Seattle, Washington. Northwest  
14 Hospital owns and operates computers, computer systems and networks used daily by  
15 the hospital in interstate and foreign commerce and communications.

16 c. Beginning at a time uncertain, but in or about July, 2004, and  
17 continuing until on or about July 7, 2005, CHRISTOPHER MAXWELL agreed and  
18 undertook to join with two others to utilize computers on the Internet to create and  
19 operate one or more Internet Relay Chat ("IRC") botnets, and to use the botnets so  
20 created silently and remotely to install adware or other unauthorized programs on  
21 compromised ("hacked") computers, without the knowledge or consent of the  
22 computers' owners. By this scheme, CHRISTOPHER MAXWELL and others  
23 intended to, and did thereby obtain commission payments from adware companies  
24 totaling approximately one hundred thousand dollars.

25 d. Internet Relay Chat ("IRC") is a text based, communications  
26 protocol for person-to-person communication ("chat") between computers on the  
27 Internet. IRC requires one or more servers and one or more clients. A client is a  
28 computer, or software running on that computer, that is used by a person to chat via

1 IRC. A server is a computer, or software running on that computer, that manages  
2 connections between the many clients and relays messages to the appropriate recipients.  
3 IRC offers the ability to have private conversations with only select clients or public  
4 conversations with multiple clients. IRC uses "channels" to determine which users are  
5 parties to which conversations. IRC supports the use of passwords, or "keys" to limit  
6 access to servers and channels. IRC also provides an administrative level of access,  
7 known as an "operator", at the channel and server level to provide configuration and  
8 policy enforcement.

9 e. An IRC network is a collection of computers communicating with  
10 each other via IRC. Generally, an IRC network includes numerous clients (between a  
11 few dozen and tens of thousands) and one or several servers (most small networks can  
12 operate with only one server, but many have several for performance and availability  
13 reasons). Servers are generally always available, while clients connect and disconnect  
14 at various times.

15 f. An IRC robot, or "bot," is a program running as an IRC client that  
16 responds autonomously to commands sent to it by the IRC server; it can thus receive  
17 commands, perform functions, and provide information back to the IRC server without  
18 human interaction at the client level. A computer infected with a malicious IRC bot  
19 and connected to an IRC server is often also referred to as a "bot," "zombie," or  
20 "drone." An IRC botnet is thus an IRC network composed primarily of IRC bots,  
21 which bots are effectively programmed to "do the bidding" of whomever has control of  
22 the IRC server.

23 g. A fundamental feature built into almost every botnet by its  
24 creator/operator is the ability to grow in size by spreading to new computers. This  
25 spreading process involves: scanning the Internet or a local network for vulnerable  
26 computers, remotely exploiting those computers, causing the exploited computer to  
27 install a copy of the IRC bot, and having those new bots connect to the IRC botnet  
28 server. The initial steps of scanning for vulnerable computers is often done in a

1 random, inefficient manner. While the process is generally successful, it has the  
2 inevitable consequence of generating large amounts of network "traffic," particularly  
3 within local networks. This increased local network traffic is often enough to interrupt  
4 normal network communications. In some cases, the interruption is complete and even  
5 the spreading botnet is prevented from functioning.

6 h. "Adware" is computer software that displays advertisements.  
7 Adware companies make money by selling advertising exposure for products or  
8 services to the company or individual that is marketing those products or services. To  
9 enhance the value of their service - displaying advertisements - adware companies seek  
10 to increase the number of computers that run their software. One strategy involves  
11 "affiliate marketing" programs, whereby the adware companies offer to pay  
12 commissions to software developers who cause users to install the adware. Generally,  
13 this takes the form of software developers "bundling" the adware with other software  
14 that is attractive to end-users. Examples include peer-to-peer file sharing programs,  
15 free screen savers, and desktop wallpaper programs. The adware companies provide  
16 the affiliates with installation programs, or "installers" for the adware that includes  
17 unique codes that attribute each installation to the particular software developer.  
18 Adware installers can sometimes be "silent", meaning that they run without user  
19 interaction or any noticeable user interface. Silent installers are provided to affiliates  
20 with the understanding that the affiliates' applications will obtain end user consent -  
21 usually by means of displaying an End User License Agreement - before running the  
22 silent installer.

23 i. Hackers can abuse this system by fraudulently becoming affiliates,  
24 and then running silent adware installers remotely on computers they have  
25 compromised, or hacked, without the knowledge or permission of the computer's  
26 owner. The computer that has been compromised then transmits the unique code,  
27 attributing the adware installation to the hacker, and thereby earning him/her  
28 commission payments. Botnets can be utilized to this end, with the result that adware



1 is silently and remotely installed on all of the compromised bot computers. By  
2 coupling adware with IRC bots, hackers can operate ever-growing botnets that generate  
3 ever-increasing adware installation commission profits as the botnet spreads.

4 j. Using the techniques described above, CHRISTOPHER MAXWELL  
5 and others knowingly and intentionally created, controlled and operated one or more  
6 botnets, and used the same to install unauthorized programs and adware on thousands  
7 of computers used in interstate communications and commerce, and obtained thereby  
8 thousands of dollars in commission payments from adware companies for those  
9 unauthorized installations. The IRC botnet created by CHRISTOPHER MAXWELL  
10 and his coconspirators included at times more than twenty thousand client computers  
11 used in interstate communications, and one or more server computers.

12 k. Specifically, CHRISTOPHER MAXWELL and others undertook the  
13 following actions to effect and further the conspiracy:

14 1) CHRISTOPHER MAXWELL and his coconspirators added client  
15 computers to their IRC network by remotely compromising, or "hacking" into  
16 computers that were owned and operated by others, without the knowledge or consent  
17 of the computers' owners;

18 2) After having remotely compromised computers, CHRISTOPHER  
19 MAXWELL and his coconspirators remotely installed on those compromised  
20 computers a malicious IRC client program, with the intended result that the IRC clients  
21 were programmed to respond autonomously to commands sent to them via the IRC  
22 servers created and controlled by CHRISTOPHER MAXWELL and his coconspirators;

23 3) The malicious code with which CHRISTOPHER MAXWELL and  
24 his coconspirators infected the individual IRC bots enabled and commanded those bots  
25 repeatedly to seek out or scan for and compromise other computers, thereby  
26 contributing to the spreading of the botnet to new and previously uninfected computers.  
27 This scanning activity had the effect of simultaneously limiting or even preventing the  
28

1 compromised computers from functioning normally and properly in accordance with the  
2 intent and directives of their legitimate owners and operators;

3 4) CHRISTOPHER MAXWELL and his coconspirators used their  
4 botnet intentionally to cause and command compromised computers surreptitiously to  
5 install adware on computers used in interstate communications without the knowledge  
6 or consent of the computers' owners, and without the knowledge of the adware  
7 companies that the adware would be installed surreptitiously and by hacking the  
8 computers of others without their knowledge or consent;

9 5) CHRISTOPHER MAXWELL and his coconspirators commanded  
10 the compromised computers on which the botnet had installed adware to register those  
11 installations with adware companies, which then generated profits by way of illicit  
12 commission payments to CHRISTOPHER MAXWELL and/or his coconspirators;

13 6) CHRISTOPHER MAXWELL and his coconspirators received  
14 commissions totaling approximately one hundred thousand dollars (\$100,000.00),  
15 consequent to the surreptitious and unauthorized installation of adware by and through  
16 their botnet;

17 7) CHRISTOPHER MAXWELL and his coconspirators also hacked  
18 into computers that belonged to others for the purpose of using them as servers for their  
19 IRC botnet. MAXWELL and his coconspirators would accomplish this by using a  
20 variety of remote exploits to gain unauthorized access to remote computers, and then  
21 surreptitiously install IRC server software on those computers without the knowledge or  
22 consent of those computer's owners. Because a high-powered computer was needed to  
23 perform the functions of an IRC Server, MAXWELL and his coconspirators often  
24 targeted high-powered computers that were part of institutional computer networks,  
25 including those of large universities. The surreptitious use of those compromised  
26 computers as illicit botnet IRC servers necessarily impaired and disrupted the normal  
27 functions and operations of the compromised computers;

1           8) CHRISTOPHER MAXWELL and his coconspirators acted  
2 intentionally to avoid detection and disruption of their illicit IRC servers by repeatedly  
3 moving the servers from one computer to another. When doing so, MAXWELL and  
4 his coconspirators would also change the Domain Name Service ("DNS") sub-domain  
5 record, which had been previously programmed into the bots, to "point to" or resolve  
6 to the new server's IP address. This change in the sub-domain record enabled the bots  
7 to find the relocated IRC server at its new location;

8           9) CHRISTOPHER MAXWELL and his coconspirators configured or  
9 commanded the bots that were part of their botnet to connect to a designated IRC  
10 channel on a specified IRC server, and to "wait" there for further commands.  
11 CHRISTOPHER MAXWELL and his coconspirators would, at their discretion,  
12 connect to the IRC channel and configure persistent commands, that would be received  
13 and executed by every bot as it connected to the channel. This system would allow the  
14 botnet to operate continuously without constant interaction by CHRISTOPHER  
15 MAXWELL and his coconspirators;

16          10) CHRISTOPHER MAXWELL and his coconspirators intentionally  
17 caused damage - that is, impaired the integrity or availability of data, a program, a  
18 system, or information - in each instance in which they compromised a protected  
19 computer without the knowledge or consent of that computer's owner, whether the  
20 compromised computer was one that was made a bot or an IRC server for the botnet;

21          11) On or about July 16, 2004, CHRISTOPHER MAXWELL created  
22 a login account with DNSMadeEasy, a company that provides free sub-domain name  
23 accounts. CHRISTOPHER MAXWELL created the account "sasserpwn" using the  
24 email address "donttrip31337@cashette.com";

25          12) On a date uncertain, but between July 16, 2004, and January 9,  
26 2005, CHRISTOPHER MAXWELL created two sub-domain name entries:  
27 "dust.page.us" and "test0r.server.us". CHRISTOPHER MAXWELL also  
28 programmed these two names into the source code of the IRC bot program that

1 MAXWELL and his coconspirators had created. The name "dust.page.us" was then  
2 used by CHRISTOPHER MAXWELL and his coconspirators to direct compromised  
3 computers to a file transfer protocol ("FTP") server containing a copy of the malicious  
4 program, which compromised computers were directed to download and execute.  
5 CHRISTOPHER MAXWELL used the name "test0r.server.us" to direct bot computers  
6 to the IRC server or servers MAXWELL and his coconspirators used to maintain and  
7 control the botnet;

8           13) On or about January 9, 2005, the botnet created and controlled by  
9 CHRISTOPHER MAXWELL and his coconspirators remotely compromised and  
10 exploited the computer systems and network of Northwest Hospital, in Seattle, WA.  
11 The botnet was designed to cause damage - that is, to impair the integrity or availability  
12 of data, a program, a system, or information stored on the Northwest Hospital  
13 computer system and network - by causing the installation of adware on victim  
14 computers, and also by causing victim computers to further spread the botnet by  
15 scanning the network for other vulnerable computers, remotely exploiting them,  
16 causing them to install a copy of the IRC bot, and having those new bots connect to the  
17 IRC server. The network traffic that resulted therefrom interrupted normal network  
18 computer communications of Northwest Hospital, with consequences to numerous  
19 hospital systems including, but not limited to, the hospital's surgical system, patient  
20 financial system, information management system, diagnostic imaging services, and  
21 laboratory services. Losses to Northwest Hospital as a result were in excess of  
22 \$5,000.00, and have been estimated by the hospital to total one hundred fourteen  
23 thousand dollars (\$114,000.00). The interruptions caused to Northwest Hospital's  
24 normal network communications also caused the modification or impairment, or  
25 potential modification or impairment of the medical diagnosis, treatment, or care of one  
26 or more of its patients, due to delays in providing information to physicians, delays in  
27 timely communicating diagnostic information, delays in processing laboratory test  
28

1 results, delays in scheduling surgery, and the temporary loss of critical computers in  
2 ICU hospital rooms.

3           14) On a date uncertain, but in or about March, 2005,  
4 CHRISTOPHER MAXWELL compromised the security of, and intruded upon a  
5 computer having the IP address \*\*.\*\*\*.79.10 that was owned by The Planet, an  
6 Internet service provider located in Dallas, Texas, and leased to one of their customers.  
7 After gaining unauthorized access to the computer at The Planet, MAXWELL remotely  
8 and surreptitiously installed IRC server software on that computer to allow him to  
9 operate and control a botnet using that computer.

10           15) On or about March 16, 2005, CHRISTOPHER MAXWELL  
11 configured the sub-domain name "test0r.server.us" to direct traffic to the IP address of  
12 the compromised computer at The Planet. In doing so, MAXWELL caused computers  
13 infected with the IRC bot program to establish persistent communications with the IRC  
14 server, allowing him to issue commands to all connected bot computers via IRC.

15           16) During the period from July 2004 to June 2005, the IRC botnet/s  
16 created and controlled by CHRISTOPHER MAXWELL (aka "donttrip"), gained  
17 unauthorized access to, and infected with malicious bot code at least 407 computer  
18 hosts (distinct IP addresses) belonging to the United States Department of Defense,  
19 including computer hosts that were part of the Headquarters, 5th Signal Command in  
20 Manheim, Germany, and others that were part of the Directorate of Information  
21 Management, Fort Carson, Colorado. The United States Department of Defense has  
22 estimated their costs to identify, rebuild, and reconfigure the infected computers to total  
23 one hundred thirty-eight thousand dollars (\$138,000.00).

24  
25           9. Non-Prosecution of Additional Offenses. As part of this Plea Agreement,  
26 the United States Attorney's Office for the Western District of Washington agrees not  
27 to prosecute Defendant for any additional offenses known to it as of the time of this  
28 Agreement that are based upon evidence in its possession at this time, or that arise out

1 of the conduct giving rise to this investigation. In this regard, Defendant recognizes  
2 that the United States has agreed not to prosecute all of the criminal charges that the  
3 evidence establishes were committed by Defendant solely because of the promises made  
4 by Defendant in this Agreement. Defendant acknowledges and agrees, however, that  
5 for purposes of preparing the Presentence Report, the United States Attorney's Office  
6 will provide the United States Probation Office with evidence of all relevant conduct  
7 committed by Defendant.

8  
9 10. Acceptance of Responsibility. The United States acknowledges that if  
10 Defendant qualifies for an acceptance of responsibility adjustment pursuant to USSG §  
11 3E1.1(a) and if the offense level is sixteen (16) or greater, Defendant's total offense  
12 level should be decreased by three (3) levels pursuant to USSG §§ 3E1.1(a) and (b),  
13 because Defendant has assisted the United States by timely notifying the authorities of  
14 his intention to plead guilty, thereby permitting the United States to avoid preparing for  
15 trial and permitting the Court to allocate its resources efficiently.

16  
17 11. Loss Amount. The United States and Defendant agree that the correct  
18 amount of the loss is between two hundred thousand dollars (\$200,000.00) and four  
19 hundred thousand dollars (\$400,000.00) for purposes of USSG § 2B1.1(b)(1).

20  
21 12. Voluntariness of Plea. Defendant acknowledges that he has entered into  
22 this Plea Agreement freely and voluntarily, and that no threats or promises, other than  
23 the promises contained in this Plea Agreement, were made to induce Defendant to enter  
24 this plea of guilty.

25  
26 13. Statute of Limitations. In the event that this Agreement is not accepted by  
27 the Court for any reason, or Defendant has breached any of the terms of this Plea  
28 Agreement, the statute of limitations shall be deemed to have been tolled from the date

1 of the Plea Agreement to: (1) 30 days following the date of non-acceptance of the Plea  
2 Agreement by the Court; or (2) 30 days following the date on which a breach of the  
3 Plea Agreement by Defendant is discovered by the United States Attorney's Office.  
4

5 14. Post-Plea Conduct. Defendant understands that the terms of this Plea  
6 Agreement apply only to conduct that occurred prior to the execution of this  
7 Agreement. If, after the date of this Agreement, Defendant should engage in conduct  
8 that would warrant an increase in Defendant's adjusted offense level or justify an  
9 upward departure under the Sentencing Guidelines (examples of which include, but are  
10 not limited to: obstruction of justice, failure to appear for a court proceeding, criminal  
11 conduct while pending sentencing, and false statements to law enforcement agents, the  
12 probation officer or Court), the United States is free under this Agreement to seek a  
13 sentencing enhancement or upward departure based on that conduct.  
14

15 15. Forfeiture. Defendant agrees to forfeit to the United States all of his  
16 right, title, and interest in any property constituting, or derived from, any proceeds the  
17 defendant obtained directly or indirectly as a result of the offenses of intentionally  
18 causing and attempting to cause damage to a protected computer and conspiracy to do  
19 so, which is subject to forfeiture pursuant to Title 18, United States Code, Section  
20 982(a)(2)(B), including but not limited to the funds in the following accounts seized by  
21 the Federal Bureau of Investigation on July 7, 2005 and September 19, 2005:

- 22 a. All Funds Held in Account Number \*\*\*\*\*5225 at Paypal, in  
23 the Name of CHRISTOPHER MAXWELL;  
24 b. All Funds Held in Account Number \*\*\*\*\*0129 at Wells Fargo, in the  
25 Name of CHRISTOPHER MAXWELL;  
26 c. All Funds Held in Account Number \*\*\*\*\*9657 at Wells Fargo, in the  
27 Name of CHRISTOPHER MAXWELL.  
28

1 Defendant further agrees to forfeit, relinquish and abandon to governmental  
2 authorities all of his right, title, and interest in the following computer, used as an  
3 instrumentality in the commission of the offenses to which he is pleading guilty:

4 A generic black and red tower computer, with a transparent side  
5 panel. This computer contains two hard drives. The first is a Seagate  
6 Barracuda ATA II drive, model number ST330630A, bearing serial  
7 number 3CK034H, with a labeled capacity of 30.6 gigabytes. The second  
8 drive is a Western Digital drive, model number WD1200, bearing serial  
9 number WMA8C4620975, with a labeled capacity of 120.0 gigabytes.

10 The computer was seized from the bedroom of Christopher Maxwell  
11 during the execution of a search warrant at his residence on July 7, 2005.  
12

13 Defendant agrees to fully assist the United States in the forfeiture of the listed  
14 assets and to take whatever steps are necessary to pass clear title to the United States,  
15 including but not limited to: surrendering title and executing any documents necessary  
16 to effectuate such forfeiture; assisting in bringing any assets located outside the  
17 United States within the jurisdiction of the United States; and taking whatever steps are  
18 necessary to ensure that assets subject to forfeiture are not sold, disbursed, wasted,  
19 hidden, or otherwise made unavailable for forfeiture. Defendant agrees not to file a  
20 claim to any of the listed property in any civil forfeiture proceeding, administrative or  
21 judicial, which may be initiated.  
22

23 // // // //

24 // // // //

25 // // // //

26 // // // //

27 // // // //

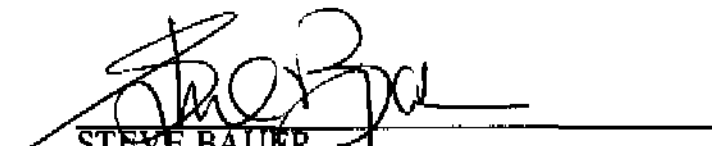
28



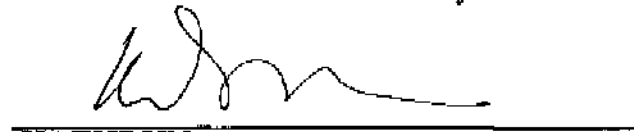
1        16. Completeness of Agreement. The United States and Defendant  
2 acknowledge that these terms constitute the entire Plea Agreement between the parties.  
3 This Agreement only binds the United States Attorney's Office for the Western District  
4 of Washington. It does not bind any other United States Attorney's Office or any other  
5 office or agency of the United States, or any state or local prosecutor.

6  
7 Dated this 4<sup>th</sup> day of May, 2006.

8  
9  
10   
11 CHRISTOPHER MAXWELL  
12 Defendant

13   
14 STEVE BAUER  
15 Attorney for Defendant

16   
17 CARL BLACKSTONE  
18 Assistant United States Attorney

19   
20 KATHRYN A. WARMA  
21 Assistant United States Attorney